First revised copy issued October 2009
Replaces the October 2008 version
Approved by the Board of Directors on October 15, 2009
Revised on April 14, 2015

TABLE OF CONTENTS

SECTION 1

DEFINITIONS

Account: A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

Annual Report: See Section 9.

Board of Directors: The Company's board of directors, or if the Company does not have a board of directors, a designated employee at the level of senior management.

Covered Account: An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

Consumer Report: A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 *et seq*.

Credit: The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

Creditor: A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit.

Customer: A person that has a Covered Account with a Creditor or a financial institution.

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

Identifying Information: A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

Notice of Address Discrepancy: A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

Red Flag: See Section 3.

Readily Available Biographical Information: Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

Service Provider: A provider of a service directly to a financial institution or Creditor.

SECTION 2

STATEMENT OF CORPORATE POLICY

The policy of Great Lakes Comnet, Inc. and its subsidiary company Comlink, LLC is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 *et seq.*, and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to Carol Thelen, Director of Compliance at 517-679-7513.

- The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:
  Carol Thelen, Compliance Director
  Paul Bowman, CEO
  Ryan Thelen, Controller
  John Summersett, COO

- The Company's Board of Directors Approved this first revised Manual on October 15, 2009 and replaces the original manual issued in October 2008.

SECTION 3

WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents.
- Unusual use or suspicious activity related to a Covered Account.
- Presentation of suspicious personal identification information.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

SECTION 4

IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts, taking into consideration:

- The methods of opening Accounts;
- The methods of access to Accounts; and
- Previous experiences with Identity Theft.

SECTION 5

OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);

2. Detect Red Flags (see Section 6);

3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and

4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

SECTION 6

IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not open a Covered Account or provide any service until it is able to satisfactorily identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the opening of the Covered Account on hold until it can satisfactorily resolve the Red Flag.

A. Opening of Covered Accounts for Personal, Family or Household Purposes.

1. Required Information: When a prospective Customer seeks to open a Covered Account for residential service (i.e., for personal, family or household purposes), the Company will ask for the following from the prospective Customer:

   - name;
   - address;
   - birth date;
   - an unexpired government-issued identification bearing a photograph, such as a driver's license or passport.

   The Company will also encourage (but not require) Customers to establish passwords as a means of protecting against potential future Identity Theft.

   The Company will encourage Customers who establish passwords not to use Readily Identifiable Biographical Information.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation.

a. The Company will make a photocopy of the prospective Customer's identification, and will inspect the identification for any signs of falsification, such as:

- misspellings;
- a photo that does not resemble the prospective Customer;
- inconsistencies in color, texture or images (such as erasures or smudges);
- raised edges around a photograph indicating the placement of a second photograph over an original photograph;
- card wear inconsistent with date of issuance (such as an identification that appears new but bears an issuance date of many years);

b. Address Discrepancies.

If a prospective Customer provides an address to the Company that does not match the prospective Customer's identification, the Company will verify the validity of the prospective Customer's address. The following are examples of methods that the Company may utilize:

- If the prospective Customer recently moved to the area, the Company will request proof of the recent move.
- The Company may choose to order a Consumer Report with respect to the prospective Consumer as a tool to confirm identity. Before ordering a Consumer Report, the Company will obtain the

prospective Customer's written approval (see Appendix 3). The Company may quiz the prospective Customer regarding non-public information contained therein. The Company may also choose to employ the services of a third-party Identity Theft detection agent.

c. The Company will create a record of the means used to verify a Customer's identity. The Company will retain such record until 5 years after the Account is closed. Upon disposal, the Company will completely destroy the record.

B. Opening of Business Accounts.

For a prospective business Customer, the Company will require documents to verify the existence of the business. Such documents may include:

- Articles of Incorporation or Articles of Limited Liability Company and evidence of filing of same with the Michigan Department of Labor and Economic Growth.
- Partnership agreement.
- Trust instrument.

A sole proprietorship may use an "assumed name" document filed with the Department of Labor and Economic Growth, or the personal information of the sole proprietor.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts.

1. Suspicious Documents and Personal Identifying Information.

   a. Information on the identification is inconsistent with information provided by the person opening a new Covered Account.

   b. Information on the identification is inconsistent with readily accessible information, such as a signature on a check.

   c. Documentation that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

   d. An address not matching any address in a Consumer Report;

   e. Documents provided for identification appear to have been altered or forged (discussed above).

2. Unusual Use of, or Suspicious Activity Related to, the Covered Account.

   a. A Covered Account is used in a manner inconsistent with established patterns of activity.

   b. Usage of a Covered Account that has been inactive for a reasonably lengthy period of time.

   c. A Customer advises that the Customer is not receiving monthly bills from the Company.

   d. A Customer advises of unauthorized charges or transactions in connection with a Covered Account.

3. The Company receives notice from a Customer, a victim of Identity Theft, law enforcement, or any other person that it may have opened an Account for a person engaged in Identity Theft.

4. If the Company uses a Consumer Report—

   a. The report contains a fraud or active duty alert.

   b. A consumer reporting agency provides a notice of credit freeze in response to a request for a Consumer Report.

   c. A consumer reporting agency provides a Notice of Address Discrepancy.

   d. A Consumer Report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a prospective Customer.

   e. A recent and significant increase in the volume of inquiries.

   f. An unusual number of recently established Credit relationships.

   g. A material change in the use of Credit, especially with respect to recently established Credit relationships.

   h. The social security number is associated with a deceased person.

   If a Consumer Report specifies a telephone number to be used for identity verification purposes, the Company will contact the consumer using the specified telephone number.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

PROTECTION OF EXISTING ACCOUNTS

The Company has policies and procedures in place to safeguard customer proprietary network information (CPNI). The Company will continue to utilize its CPNI policies procedures as a safeguard against unauthorized access to Customer CPNI, including pre-texting. Pre-texting is the practice of obtaining call record detail and other CPNI under false pretenses. The Company also monitors suspicious transactions, and verifies change of address requests in accordance with its CPNI Compliance Manual.

The Company updates its Manual to account for changes in law, and it contains all essential information and forms to ensure the Company's compliance with CPNI regulations.

The Company will continue to follow its CPNI Compliance Manual as a means of preventing Identity Theft. The Company will also continue to improve its Identity Theft Prevention Program based on its experience with past incidents of Identity Theft, and new methods of committing Identity Theft of which it becomes aware.

The Company treats the following as Red Flags—

- Alerts, notifications, or other warnings from consumer reporting agencies or Service Providers;
- Suspicious address changes;
- The unusual use of, or other suspicious activity related to, a covered Account; and
- Notice from Customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with a Covered Account.

SECTION 7

PREVENTING AND MITIGATING IDENTITY THEFT

The Company will respond appropriately when it detects a Red Flag. In determining how to respond, the Company will consider aggravating factors that may heighten the risk of Identity Theft.

Appropriate responses include one or more of the following depending on the circumstances:

- Monitoring a Covered Account;
- Contacting the Customer;
- Changing passwords or security codes that permit access to a Covered Account;
- Reopening a Covered Account with a new account number;
- Declining to open a Covered Account for a prospective Customer;
- Closing an existing Covered Account
- Not collecting on a Covered Account; or
- Notifying law enforcement (see Section 10 of CPNI Compliance Manual).

SECTION 8

UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The Company will update this Program periodically to reflect changes in risks to Customers or to the safety and soundness of the Company from Identity Theft.

In updating this Program, the Company will consider the following:

- The Company's experiences with Identity Theft.
- Changes in methods with which Identity Theft is committed.
- Changes in methods to detect, prevent, and mitigate Identity Theft.
- Changes in the types of Accounts that the Company offers or maintains.
- Changes in the Company's business arrangements, such as mergers, acquisitions, alliances, joint ventures, and Service Provider arrangements.

SECTION 9

ANNUAL REPORT

The Company will designate a person to be responsible for preparing an Annual Report to the Board of Directors, appropriate committee of the Board, or a designated senior-level manager.

The Annual Report will address at least the following:

- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts.
- The effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft with respect to existing Covered Accounts.
- Arrangements with Service Providers.
- Significant incidents involving Identity Theft and management's response.
- Recommendations for material changes to the Company's Identity Theft Prevention Program.

The Annual Report will be in a format similar to that contained in Appendix 1.

SECTION 10

SERVICE PROVIDERS

To the extent that the Company engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the Company will ensure that the Service Provider has its own Identity Theft Prevention Program to detect and address Red Flags.

The Company is ultimately responsible for complying with Red Flag rules even if it outsources Account-related activity to a Service Provider.

SECTION 11

USE OF CONSUMER REPORTS

To the extent that the Company uses Consumer Reports in the opening of a new Covered Account, it will comply with this Section 11.

If the Company receives a Notice of Address Discrepancy from a consumer reporting agency, the Company must form a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report.

The Company will do one or more of the following to determine whether it has a reasonable belief that the Consumer Report relates to the prospective Customer about whom it has requested the report:

- Compare the information in the Consumer Report with information the Company uses to verify the prospective Customer's identity.
- Compare the information in the Consumer Report provided by the consumer reporting agency with information the Company obtains from third-party sources.
- Verify with the prospective Customer.

If the Company has reasonably confirmed that an address relates to the prospective Customer about whom it has requested the report, it must furnish the address for the prospective Customer to the consumer reporting agency from whom it received the Notice of Address Discrepancy.

SECTION 12

DISCIPLINARY ACTION

Any failure to follow this Manual will result in appropriate disciplinary action in accordance with established Company disciplinary policies. Such failures shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. The Company will also require additional training to ensure future compliance.

APPENDIX 1

ANNUAL REPORT FORM

To be completed by the Board of Directors, appropriate committee of the Board of Directors, or a designated senior-level manager.

ANNUAL REPORT FOR _____

This Annual Report constitutes _____ Company's (Company) obligation under the Federal Trade Commission's (FTC) regulations and guidelines, 16 CFR Part 681, to produce an Annual Report to address the Company's compliance with the FTC's Red Flag regulations.

1. Effectiveness of Policies and Procedures

a. Opening of Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts:

b. Existing Covered Accounts

The Company provides the following report regarding the effectiveness of the Company's policies and procedures in addressing the risk of Identity Theft in connection with existing Covered Accounts:

2. Arrangements with Service Providers

The Company [does/does not] outsource some services to third party Service Providers related to Covered Accounts. [If the Company "does," list them and state:] The Company has taken the following measures to ensure that its Service Provider(s) have Identity Theft Prevention Program(s) to detect and address Red Flags:

3. Significant Incidents Involving Identity Theft

The Company reports the following significant incidents involving Identity Theft and management's response:

4. Recommendations for Material Changes to the Program

The Company should consider the following changes to its Identity Theft Prevention Program.

_____ Title_____
Name

Date: _____

APPENDIX 2

EMPLOYEE VERIFICATION OF RED FLAG COMPLIANCE MANUAL REVIEW

Red Flag
Employee Acknowledgment

Employee Name:_____

I have reviewed the Company's Red Flag and Address Discrepancies Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

_____
Employee Signature

_____
Date

APPENDIX 3

SAMPLE FORM FOR CREDIT REPORT AUTHORIZATION